Вісник ЛДУБЖД
Bulletin of Lviv State University of Life Safety
https://journal.ldubgd.edu.ua/index.php/Visnuk
ISSN 2078-4643 (print), ISSN 2708-1389 (online)

UDC 004.056:005.8
DOI: 10.32447/20784643.33.2026.14
This article is an Open Access article distributed under the terms and conditions of the Creative Commons Attribution 4.0 (CC BY 4.0) License (http://creativecommons.org/licenses/by/4.0/).

О. А. Нємкова, Т. І. Коробейнікова, М. К. Русинко, С. Т. Масник
Національний університет "Львівська політехніка", м. Львів, Україна
ORCID: https://orcid.org/0000-0003-0690-2657 – О. А. Нємкова
https://orcid.org/0000-0003-2487-8742 – Т. І. Коробейнікова
https://orcid.org/0000-0002-6808-3506 – М. К. Русинко
https://orcid.org/0009-0002-5797-9056 – С. Т. Масник
olena.a.niemkova@lpnu.ua

МОНІТОРИНГ АКТИВНОСТІ БАЗ ДАНИХ КОРПОРАТИВНИХ СИСТЕМ ЗАСОБАМИ SIEM

Цифрова трансформація та стрімкий розвиток інформаційних технологій призводять до зростання ризиків конфіденційності, цілісності та доступності корпоративних даних, зокрема в системах командної взаємодії та управління проєктами. Забезпечення належного рівня інформаційної безпеки в таких умовах вимагає не лише застосування традиційних засобів захисту, а й використання сучасних аналітичних рішень, здатних виявляти, корелювати та оперативно реагувати на загрози в режимі реального часу. Відтак постає проблема забезпечення ефективного моніторингу та своєчасного реагування на інциденти інформаційної безпеки, що зумовлює необхідність впровадження систем керування подіями та інформаційною безпекою (далі – SIEM) як ключового елемента сучасної архітектури кіберзахисту.

Метою роботи є розробка конфігурації SIEM-системи для активізації журналювання системи керування базами даних для відстеження підозрілої діяльності, модифікуючих запитів та помилок. Для цього розглянуто використання Splunk Enterprise як платформи для централізованого журналювання та кореляції подій і запитів у базах даних MySQL. Проаналізовано сучасні підходи до захисту корпоративної інформації, зокрема комерційної таємниці й об'єктів інтелектуальної власності, що обробляються в корпоративних інформаційних системах. Охарактеризовано особливості конфігурації запропонованого рішення, яке забезпечує ефективне збирання, зберігання та аналіз подій інформаційної безпеки.

Запропоновано конфігурацію SIEM-системи для моніторингу активності баз даних, яка дає змогу не лише виявляти підозрілі та аномальні запити, але й скорочувати середній час реагування на інциденти завдяки використанню автоматизованих сповіщень та аналітики в реальному часі. З'ясовано, що ефективна імплементація підсистеми моніторингу активності баз даних здатна мінімізувати наслідки кібератак, запобігати витоку даних і підвищувати загальний рівень інформаційної безпеки підприємства. Оцінено вплив упровадження SIEM на продуктивність корпоративних інформаційних систем і встановлено, що коректна конфігурація моніторингу не спричиняє помітного зниження їх ефективності.

Практичне значення отриманих результатів полягає у можливості застосування запропонованих рекомендацій як у комерційних структурах, так і в державних установах для забезпечення ефективного контролю за циркуляцією та обробкою конфіденційних даних. Отримані результати можуть бути використані як основа для подальших досліджень, спрямованих на оптимізацію конфігурацій SIEM-систем та інтеграцію методів машинного навчання для прогнозної аналітики інформаційної безпеки.

Ключові слова: цифрова трансформація; інформаційна безпека; корпоративні бази даних; моніторинг запитів до баз даних; SIEM; Splunk Enterprise.

E. A. Niemkova, T. I. Korobeynikova, M. K. Rusynko, S. T. Masnyk
National University "Lviv Polytechnic", Lviv, Ukraine

MONITORING DATABASE ACTIVITY IN CORPORATE SYSTEMS USING SIEM TOOLS

Digital transformation and the rapid development of information technologies have significantly increased the risks to the confidentiality, integrity, and availability of corporate data, particularly in systems for team management and collaboration. Ensuring proper information security under such conditions requires not only traditional protection mechanisms but also advanced analytical tools capable of identifying, correlating, and responding to threats in real time. Therefore, the problem of ensuring effective monitoring and timely response to information security incidents necessitates the implementation of Security Information and Event Management (hereinafter referred to as SIEM) systems as a key component of modern cybersecurity architecture.

The aim of the work is to develop a SIEM system configuration to activate database management system logging to track suspicious activity, modifying queries, and errors. For this, the use of Splunk Enterprise is considered as a platform for centralized logging and correlation of events and queries in MySQL databases.. The paper reviews current methods of protecting corporate information, including trade secrets and intellectual property, which are processed within corporate information systems. The features and configuration of the proposed monitoring solution are characterized, ensuring efficient collection, storage, and analysis of security events.

A SIEM system configuration for database activity logging is proposed, which not only enables the detection of suspicious and anomalous queries but also reduces the average incident response time through real-time alerting and automation capabilities. It has been found that the effective implementation of a database activity monitoring subsystem can minimize the consequences of cyberattacks, prevent data leakage, and improve the overall level of enterprise information security. Furthermore, the impact of SIEM implementation on the performance of corporate information systems has been assessed, showing that proper monitoring configuration does not cause noticeable system performance degradation.

The practical significance of the obtained results lies in the possibility of applying the proposed recommendations both in commercial enterprises and in public institutions to ensure effective control over the circulation and processing of confidential data. The results can also serve as a basis for further research aimed at optimizing SIEM configurations and integrating machine learning techniques for predictive security analytics.

Keywords: digital transformation; information security; corporate databases; database query monitoring; SIEM; Splunk Enterprise.

Вступ

Проблеми кібербезпеки корпоративних інформаційних систем та баз даних (далі – БД) привертають дедалі більшу увагу дослідників у зв'язку зі стрімким розвитком технологій та зростанням кількості кіберінцидентів. Сучасні наукові праці активно досліджують методи та засоби захисту інформації в корпоративних середовищах, зокрема через інтеграцію рішень класу SIEM, що дає можливість швидко аналізувати величезні обсяги даних журналів безпеки сучасних мереж [1]. Дослідження з цієї тематики акцентують увагу на розробці архітектури системи, процесу створення та оптимізації правил детектування, а також аналізують ефективність системи у виявленні реальних кіберзагроз [2]. З погляду світової тенденції до автоматизації моніторингу та використання інтелектуальних систем аналізу подій, використання SIEM розглядають для підвищення точності та швидкості виявлення вторгнень шляхом інтеграції технологій машинного навчання (ML). Таким чином, SIEM дозволяє не лише реєструвати порушення, а й своєчасно на них реагувати, скорочуючи час на обробку інцидентів [3].

Водночас, аналіз наукової літератури засвідчив, що недостатньо уваги приділено особливостям моніторингу активності корпоративних БД, що використовуються у системах менеджменту командної роботи, зокрема в контексті захисту комерційної таємниці й інтелектуальної власності.

Таким чином, актуальність і необхідність проведення подальших досліджень у зазначеній галузі зумовлена потребою розроблення та практичного впровадження конфігурації SIEM-системи для моніторингу активності корпоративних БД в системах управління командною роботою.

Загальне питання інформаційної безпеки підприємств у контексті цифрової трансформації є дуже актуальним та активно досліджується [4–6]. В умовах сьогодення цифрова інформація стає основним активом підприємств [7], а значення конфіденційних даних [8–9], комерційної таємниці та інтелектуальної власності постійно зростає [10–11]. Цифровізація суспільства, крім очевидних переваг, породжує нові виклики, що стосуються кіберзлочинності та захисту даних [12]. Управління корпоративною інформацією та захист її конфіденційності є темою численних досліджень та публікацій [13]. У цьому дослідженні автори керуються тим, що збереження таких ключових характеристик інформації, як конфіденційність, цілісність та

доступність (CIA-тріада), залишається відкритим питанням і потребує застосування комплексних засобів захисту [14–15].

Ряд авторів досліджують питання захисту інформації саме в аспекті комерційної таємниці та інтелектуальної власності [10,11, 13, 14], відзначаючи необхідність застосування внутрішніх політик та спеціалізованих технічних рішень для забезпечення безпеки та моніторингу активності. Серед засобів, які дозволяють проводити моніторинг та аналіз подій безпеки інформаційних систем, виокремлюють системи класу SIEM [17–19]. Такі системи інтегрують збір, аналіз та управління інформацією про безпеку, а також подіями безпеки у єдиний процес. Часто науковці фіксують увагу на необхідності детального моніторингу активності баз даних підприємств, зокрема використовуючи SIEM-рішення Splunk Enterprise, що забезпечує реєстрацію і аналіз подій у режимі реального часу, допомагаючи своєчасно реагувати на кіберінциденти. Хоча проблематика захисту інформації є добре вивченою, мало приділяється уваги особливостям реалізації моніторингу саме в системах менеджменту командної роботи, де дані мають особливу комерційну та інтелектуальну цінність.

Таким чином, критичний аналіз доступної літератури вказує на недостатнє висвітлення особливостей моніторингу баз даних у системах менеджменту командної роботи з позицій інформаційної безпеки, що підтверджує актуальність та необхідність подальшого дослідження.

Мета дослідження полягає у розробці конфігурації SIEM-системи для активізації журналювання системи керування базами даних для відстеження підозрілої діяльності, модифікуючих запитів та помилок.

Методи дослідження

У дослідженні застосовано комплексний підхід, який поєднує аналітичні, експериментальні та порівняльні методи, а також методи логічного аналізу та моделювання процесів.

На аналітичному етапі здійснено огляд наукових джерел і сучасних публікацій, присвячених використанню систем керування інформаційною безпекою та подіями безпеки (SIEM), а також методів моніторингу активності баз даних (Database Activity Monitoring, DAM). Проведено систематизацію основних напрямів розвитку технологій захисту корпоративної інформації та виявлено недоліки існуючих рішень.

На експериментальному етапі реалізовано модель корпоративної бази даних на платформі MySQL, яка використовувалася як тестове середовище для збору журналів запитів, помилок і повільних транзакцій. Для побудови системи моніторингу застосовано SIEM-платформу Splunk Enterprise, що забезпечила централізоване журналювання, обробку та аналіз подій безпеки. Конфігурація середовища виконувалася за допомогою розширення Splunk DB Connect, яке дозволяє інтегрувати систему керування базами даних (далі – СКБД) із системою моніторингу.

Методи логічного аналізу та моделювання процесів використано для опису архітектури системи моніторингу, визначення взаємозв'язків між компонентами SIEM і базою даних, а також для розроблення сценаріїв реагування на інциденти. Застосовано порівняльний аналіз для оцінки ефективності журналів різних типів (загального, повільних запитів, помилок, двійкового та реплікаційного), а також для визначення оптимальної конфігурації журналювання.

Оцінювання результатів проводилося шляхом емпіричного тестування продуктивності системи під час моніторингу, вимірювання часу обробки запитів та аналізу обсягу зібраних даних. Для перевірки ефективності сповіщень та виявлення інцидентів налаштовувалися автоматичні тригери, що реагували на події у журналах. Отримані результати було інтерпретовано за допомогою візуальних панелей Splunk Enterprise для подальшого аналітичного опрацювання.

Таким чином, використані методи забезпечили комплексне дослідження можливостей SIEM-систем у контексті моніторингу активності баз даних корпоративних середовищ і дали змогу сформувати практичні рекомендації щодо оптимізації їх конфігурації.

Наукова новизна отриманих результатів дослідження – вперше запропоновано спеціалізовану конфігурацію SIEM-системи Splunk Enterprise, орієнтовану саме на моніторинг активності БД у системах менеджменту командної роботи, що дозволяє суттєво зменшити час реагування на кіберінциденти.

Практична значущість результатів дослідження – можливість застосування розроблених рекомендацій підприємствами та установами як приватного, так і державного секторів для підвищення безпеки корпоративних інформаційних ресурсів.

Результати дослідження

Моделі систем управління проектами. Сучасне управління проєктами вимагає інтегрованих систем для відстеження завдань, прогресу роботи та ефективної взаємодії у команді. Водоспадна модель (англ. Waterfall) передбачає послідовне проходження етапів проєкту: вимоги, аналіз, дизайн, розробка, тестування, підтримка. Переваги цього підходу – прозорість, стабільність вимог, чітке планування термінів і витрат. Основні недоліки – негнучкість та складність змін у процесі

виконання проєкту. Гнучка модель (англ. Agile) складається з циклів розробки, в яких здійснюються дослідження, створення прототипу, розробка, тестування, реліз і моніторинг. Agile акцентує увагу на адаптивності, швидкій реакції на зміни, активній взаємодії з клієнтом. Водночас потребує високої кваліфікації команди та ускладнює точні оцінки термінів і вартості проєкту. До Agile-методик належать Scrum, Kanban, Lean та Extreme Programming (далі – XP). Scrum використовує короткі цикли роботи (спринти), Kanban орієнтований на безперервність процесу та візуалізацію завдань, Lean – на мінімізацію втрат та оптимізацію процесів, а XP – на швидке реагування на зміну вимог через ітеративне програмування.

Відомо, що більшість систем менеджменту командної роботи приділяють недостатньо уваги питанням безпеки та детального управління доступом, що створює ризики для конфіденційності даних. Вони передбачають активний обмін інформацією, значна частина якої має комерційну цінність, визначається як конфіденційна та підлягає захисту.

Захист корпоративної інформації. Корпоративна інформація має комерційну цінність, характеризується актуальністю, достовірністю та доступністю, тому потребує забезпечення конфіденційності, цілісності та доступності. Додаткові важливі властивості – спостережність та невідмовність. Комерційна таємниця – інформація, що невідома третім особам та має економічну цінність для компанії. Її захист вимагає внутрішніх нормативних актів, угод про нерозголошення, тренінгів співробітників та обмеження доступу до даних. Інтелектуальна власність охоплює права на результати інтелектуальної діяльності: авторські права, товарні знаки, комерційну таємницю. Захист передбачає реєстрацію прав, запобігання піратству, плагіату та іншим порушенням. Угода про нерозголошення юридично зобов'язує сторони зберігати конфіденційність інформації. Вона може бути односторонньою, двосторонньою або багатосторонньою, включати перелік захищених даних, умови їх використання та відповідальність за порушення.

Корпоративні БД. Корпоративні системи зазвичай використовують клієнт-серверну архітектуру з реляційними БД. Захист інформації в них забезпечується методами автентифікації та розподілом прав доступу. Критичним компонентом безпеки є ведення журналів для фіксації подій. Загальний журнал запитів реєструє всі команди; журнал повільних запитів використовують для оптимізації продуктивності; журнал помилок документує проблеми в роботі системи керування БД; двійковий журнал записує зміни даних для реплікації та відновлення; реплікаційний журнал використовується для синхронізації реплік БД.

*Моніторинг активності БД***.** Моніторинг активності БД (далі – DAM) дає змогу реєструвати й аналізувати транзакції БД, ідентифікувати порушення та виявляти аномалії в реальному часі. Основні задачі DAM:

1) відстеження привілейованих користувачів та запобігання внутрішнім загрозам;
2) моніторинг дій корпоративних додатків для виявлення зловживань доступом;
3) запобігання SQL-ін’єкціям через аналіз структури запитів.

Системи керування подіями та інформаційною безпекою

SIEM системи централізують та аналізують події безпеки, агрегуючи інформацію з усіх доступних джерел. Вони забезпечують виявлення загроз в режимі реального часу, інтегроване управління подіями безпеки та генерування звітів щодо відповідності стандартам безпеки. Сучасні SIEM-платформи використовують штучний інтелект для визначення моделей поведінки користувачів, дозволяють автоматично реагувати на загрози, а також інтегруються з DAM для глибокого моніторингу активності БД.

Порівняння SIEM та DAM. Обидві системи мають схожу архітектуру, але відрізняються за масштабами та глибиною аналізу. DAM детально аналізує транзакції БД в реальному часі, тоді як SIEM забезпечує комплексний аналіз подій в масштабах усієї корпоративної інфраструктури. SIEM має перевагу в кореляції подій різних типів і формуванні глобальної картини безпеки, тоді як DAM є більш ефективним для точкового глибокого аналізу діяльності саме в базах даних.

Отож, захист корпоративної інформації є критичним завданням для будь-якої компанії. Використання SIEM та DAM дозволяє здійснювати ефективний контроль за інформаційною безпекою, запобігати загрозам та мінімізувати ризики, пов'язані з компрометацією корпоративних даних. Корпоративні БД мають неабияку фінансову та репутаційну цінність, а їхня компрометація може нести за собою цивільно-правову, дисциплінарну, адміністративну та кримінальну відповідальність. Тож, додатково з застосуванням звичних видів захисту, необхідно вести облік користувацької активності, аби мати можливість вчасно зреагувати на інцидент.

Для демонстрування результативності систем управління інформаційною безпекою та подіями безпеки у контексті моніторингу діяльності БД використано Splunk (для

колекціонування та аналітичної агрегації даних). Робочим середовищем є БД локального клієнт-серверного вебдодатка (рис. 1) "ManagementCalendar" (за СКБД обрано MySQL).

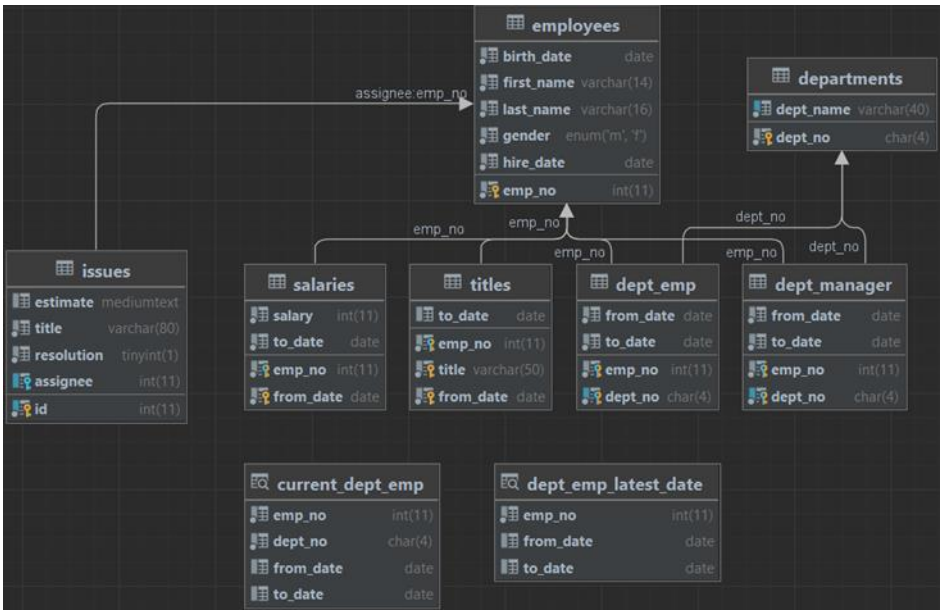

Рисунок 1 – Структура БД локального клієнт-серверного вебдодатка

Для збору даних активності БД у Splunk застосовано надбудову Splunk DB Connect – це загальне розширення БД SQL для Splunk, яке дозволяє легко інтегрувати інформацію БД із запитами та звітами Splunk. Splunk DB Connect підтримує DB2/Linux, Informix, MemSQL, MySQL, AWS Aurora, Microsoft SQL Server, Oracle, PostgreSQL, AWS RedShift, SAP SQL Anywhere, Sybase ASE, Sybase IQ та Teradata.

Додаток має чотири вкладки для задоволення максимальних потреб у взаємодії із обраною системою керування БД (Inputs використовуються для імпорту структурованих відомостей, аналізу та візуалізації; Outputs – для експорту аналітичних даних машини до застарілої БД; Lookups – для додавання значущої інформації до даних подій; SQL Explorer застосовується для створення інформаційних панелей).

Надбудова Splunk для MySQL дозволяє адміністратору програмного забезпечення Splunk збирати загальні журнали, журнали помилок і журнали повільних запитів із серверів MySQL, а також журнали продуктивності та конфігурації з локальних або віддалених БД MySQL. Є дві групи типів джерел для надбудови Splunk для MySQL – зібрані через Splunk DB Connect та зібрані через моніторинг файлів.

Після конфігурації БД, ввімкнення журналювання та забезпечення виведення журналів логування одночасно у файл і у таблицю (рис. 2 а), в директорію інсталяції Splunk додано конектор СКБД (у цьому випадку mysql-connector-java*.jar, оскільки операційною системою є Windows) (рис. 2 б). Далі конфігурація надбудови відбувається безпосередньо в графічній оболонці Splunk Enterprise, починаючи із створення нової ідентичності офіцера безпеки та надання їй відповідних повноважень.

Рисунок 2 – а) налаштування виведення журналів логування; б) до директорії Splunk додано конектор СКБД

В заданому контексті Splunk виконуватиме роль монітора та не матиме прямого впливу на використовувану БД, створювана ідентичність офіцера безпеки не потребуватиме прав на запис в таблиці БД. Ідентичність повинна мати доступ до схем information_schema, performance_schema та mysql, оскільки там міститься вся необхідна інформація щодо логування, процесів, користувачів тощо. На основі нової ідентичності виконується налаштування підключення. З метою перешкоджання порушенню цілісності адміністратором встановлюється прапорець read only. Результат діючого з'єднання зображено на рис. 3.

Рисунок 3 – Сконфігуроване підключення

Виконується налаштування запитів на отримання вхідних даних: з таблиць для загального та повільних запитів журналів та з файлу для журналу помилок. Обидва методи забезпечують отримання інформації в реальному часі або за запланованим графіком. Окрім одноразових ручних запусків створених запитів на отримання інформації та постійної присутності детекторів у фоні можна налаштувати також запуск служби за певним графіком, наприклад, щоб він запускався кожні 10 хвилин. Для своєчасного виявлення критичних помилок налаштовано пріоритетне сповіщення в реальному часі на кожен окремий рядок.

Для зручності проведення аналітичних досліджень Splunk надає три види панелей (моніторів) з можливістю задання у якості фільтрів необхідного розрізу часу, підключення та конкретного джерела отримання вхідних даних (рис. 4–6).

Перший монітор (рис. 4) дає змогу проглядати стан запитів на отримання вхідних даних та фіксує в одиницях і відсотках кількість запитів, що були неуспішними, а також показує загальну кількість викликів кожної окремої служби на визначеному відрізку часу та скільки із них завершено із помилками.

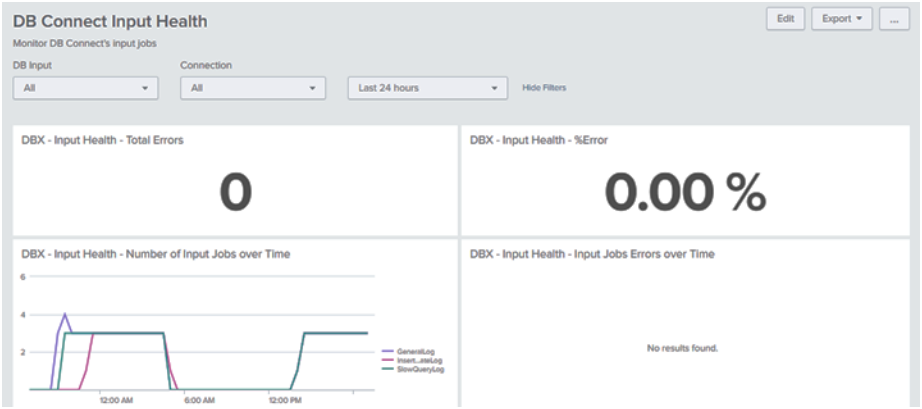

Рисунок 4 – Монітор служб вхідних даних

Наступний монітор (рис. 5) демонструє продуктивність виконуваних запитів службами та показує середній час тривалості виконання служби, розподіл часу по службах, середні тривалість запиту та пропускну здатність тощо.

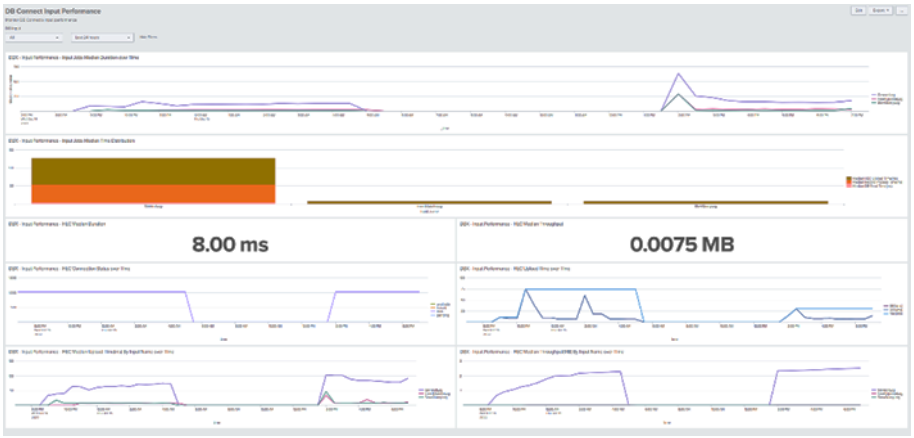

Рисунок 5 – Монітор продуктивності вхідних даних

Остання панель (рис. 6) стосується справності підключень, вказує кількість помилок при спробі клієнтського з'єднання із БД та відповідне відсоткове представлення, кореляцію активних підключень до кількості виконаних запитів, час очікування та тривалість з'єднань.

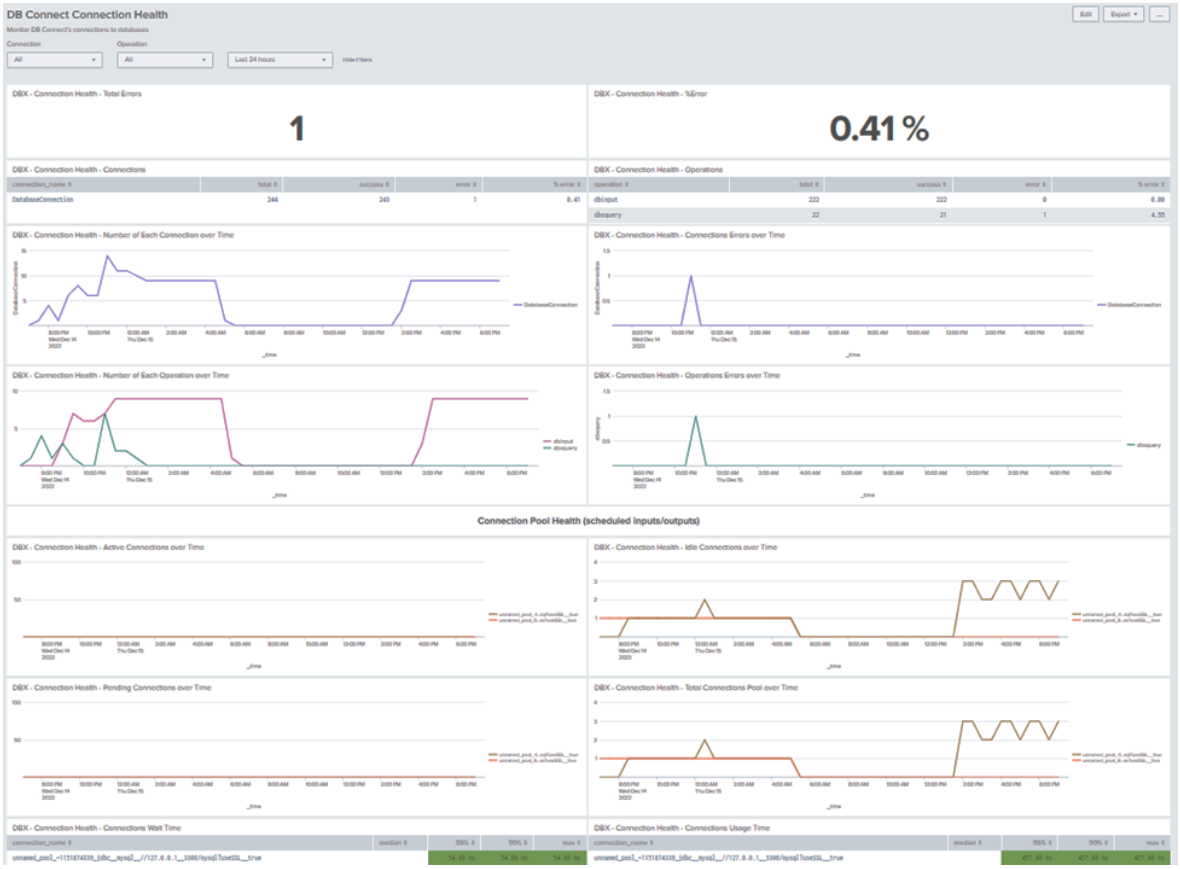

Рисунок 6 – Монітор підключень до БД

Основним результатом дослідження є процеси конфігурації та експлуатації системи керування БД та SIEM-платформи на прикладі Splunk у ролі монітора активності БД на основі інформації з таблиць та файлу журналювання в реальному часі. Можна зробити висновок, що сучасні інструменти управління інформаційною безпекою та подіями безпеки надають широкий спектр можливостей для конфігурації найрізноманітніших видів моніторингу БД, аплікацій і зовнішніх пристроїв та дозволяють акумулювати отримані відомості в повноцінні звіти з подальшим аналізом кореляції подій.

Обговорення результатів досліджень

Отримані в процесі виконання дослідження результати свідчать про доцільність застосування систем моніторингу активності баз даних та SIEM-рішень у системах менеджменту командної роботи з метою забезпечення належного рівня інформаційної безпеки.

Одним із ключових висновків дослідження є те, що стандартні підходи, такі як автентифікація користувачів або базові механізми контролю доступу, не завжди достатні для захисту конфіденційних даних у корпоративних середовищах. Особливо це стосується командних систем управління, які характеризуються високою динамікою обміну інформацією між великою кількістю учасників із різними ролями доступу. Впровадження додаткових засобів моніторингу активності, зокрема SIEM-систем, дозволяє не тільки реєструвати випадки порушень політик безпеки, але й своєчасно реагувати на такі події.

Проведений аналіз різних типів журналювання (загальний журнал запитів, журнал повільних запитів, журнал помилок, двійковий журнал) показав, що ефективність моніторингу значною мірою залежить від правильності конфігурації обраних інструментів. Встановлено, що оптимальним є використання загального журналу та журналу помилок для базового моніторингу активності, а двійковий журнал рекомендується для більш глибокого аналізу дій користувачів (наприклад, під час розслідування інцидентів або відновлення даних після атак).

Особливу увагу приділено можливостям рішення Splunk Enterprise, яке є інструментом моніторингу в даному дослідженні. З'ясовано, що ця SIEM-система забезпечує високий рівень аналітики та інтеграції даних із різних джерел, дозволяючи створювати комплексні сценарії виявлення підозрілої активності на основі кореляції подій. Водночас, наголошено, що реалізація повноцінної системи моніторингу на основі Splunk потребує врахування низки факторів, серед яких – правильна класифікація

подій, налаштування фільтрів журналів та чітке визначення політик реагування.

Важливою проблемою, що виникає під час впровадження системи моніторингу, є велика кількість даних, яка може негативно впливати на продуктивність і ускладнювати аналіз подій. Це свідчить про необхідність точного налаштування системи, ретельного відбору важливих подій для реєстрації та використання автоматизованих інструментів обробки та кореляції.

Таким чином, результати дослідження підтвердили актуальність впровадження спеціалізованих SIEM-систем у корпоративних середовищах, однак також вказали на необхідність ретельного планування, налаштування та регулярного перегляду їхніх конфігурацій. Подальші дослідження в цьому напрямку могли б бути спрямовані на оптимізацію процедур моніторингу активності баз даних з використанням штучного інтелекту та машинного навчання для зниження кількості помилкових спрацьовувань і покращення ефективності управління інформаційною безпекою.

Висновки

В результаті цього дослідження було розроблено та описано конфігурацію SIEM-системи на базі Splunk Enterprise для моніторингу активності баз даних (зокрема, MySQL) у корпоративних системах, що дає змогу відстежувати підозрілу діяльність, запити модифікації та помилки в режимі реального часу. Це рішення базується на загальних принципах налаштування журналювання та інтеграції з базами даних, забезпечуючи централізований збір, зберігання та аналіз подій безпеки.

Запропонована конфігурація системи моніторингу дає змогу виконувати аналіз активності користувачів, виявляти порушення політик безпеки та ефективно управляти інцидентами інформаційної безпеки. Таке рішення повинно сприяти зниженню ймовірності внутрішніх загроз та несанкціонованого доступу до конфіденційної інформації, а також скороченню середнього часу реагування на інциденти завдяки автоматизованим сповіщенням.

Експериментально підтверджено, що застосування описаної конфігурації посилює контроль за станом інформаційної безпеки без помітного зниження продуктивності корпоративних систем. Водночас автори сподіваються, що запропоноване рішення, завдяки основному призначенню SIEM-системи для швидкого виявлення порушень політик безпеки, сприятиме покращенню результативності виявлення інцидентів та підвищенню загального рівня безпеки роботи команди зі спільною базою даних. Крім того, визначено ключові аспекти впровадження, такі як точне налаштування журналювання, вибір оптимального обсягу даних та формування політик реагування.

Результати дослідження підтверджують ефективність використання SIEM-систем для моніторингу баз даних у корпоративних середовищах, що створює основу для подальшого розвитку технологій захисту інформації, зокрема шляхом інтеграції методів машинного навчання для прогнозної аналітики безпеки.

Список літератури:

1. Sheeraz M., Paracha M., Haque M., Durad M. and oth. Effective Security Monitoring Using Efficient SIEM Architecture. *Human-centric Computing and Information Sciences*, vol.13, Article number 23, 2023. https://doi.org/10.22967/HCIS.2023.13.023
2. Kozak M., Plichta A. Implementation of a SIEM System Using Splunk and the Enterprise Security Module and Analysis of Its Effectiveness in Detecting Cyber Threats. Proceedings of Conference: 39th ECMS International Conference on Modelling and Simulation, vol. 39, is. 1, 2025. https://doi.org/10.7148/2025-0269
3. Okamoto H. The Role of Information Security Event Management (SIEM) in Enhancing Intrusion Detection and Cybersecurity Through Machine Learning Technology. 2021. https://doi.org/10.13140/RG.2.2.35096.00003
4. Дергалюк Б. В. Вплив цифрової трансформації на забезпечення економічної безпеки підприємства. *Економічний вісник Національного технічного університету України "Київський політехнічний інститут"*, (26), 2023. С. 65-68. https://doi.org/10.20535/2307-5651.26.2023.287057
5. Крамаренко І. С., Іртищева І. О., Білоусова С. В., Іртищев О. С., & Гарагуля, А. В. Організаційно-управлінські механізми забезпечення інформаційної безпеки підприємницької діяльності в умовах цифрової трансформації економіки України. *Підприємництво та інновації*, (32), 2024. С.246-252. https://doi.org/10.32782/2415-3583/32.38
6. Польова Н., Когут Р., & Дума Ю. Напрями забезпечення безпеки підприємства в умовах цифровізації бізнесу. *Розвиток міста*, (1 (01)), 2024. С.90-94. https://doi.org/10.32782/city-development.2024.1-12
7. Шевчук А. А. Захист цифрового активу з використанням ШІ – основа безпеки країни та ефективність управління бізнес процесами в умовах цифровізації. *Цифрова економіка та економічна безпека*, (3 (12)), 2024. С.41-46. https://doi.org/10.32782/dees.12-7
8. Легомінова С. В., Щавінський Ю. В., & Будзинський О. В. Аналіз сучасних підходів до забезпечення кібербезпеки корпоративних баз даних. *Сучасний захист інформації*, (2), 2024. С.50-58. https://doi.org/10.31673/2409-7292.2024.020006

9. Бондарчук О. І., Науменко Т. С., & Товт Б. М. Розробка та впровадження інноваційних методів кібербезпеки у комп'ютерних системах. *Таврійський науковий вісник. Серія: Технічні науки*, (4), 2024. С.31-40. https://doi.org/10.32782/tnv-tech.2024.4.3

10. Бакалінська О. Сучасні тенденції правового регулювання кібербезпеки та інтелектуальна власність. *Теорія і практика інтелектуальної власності*, (5), 2022. С.82-92. URL: https://coordynata.com.ua/sucasni-tendencii-pravovogo-reguluvanna-kiberbezpeki-ta-intelektualna-vlasnist

11. Андрощук Г. Інтелектуальна власність в системі інтернет речей: економіко-правовий аспект. *Теорія і практика інтелектуальної власності*, (6), 2017. URL: https://drive.google.com/file/d/1lytwL95SQuvdNa8-d3DbMvQ51P0hmeW/view

12. Калашнікова Л. В., & Ярова Л. Цифровізація соціальних відносин: теоретичне обгрунтування та емпірична верифікація. Каравела. 2023. URI: http://elibrary.kdpu.edu.ua/xmlui/handle/123456789/10687

13. Чубаєвський В. Методи управління корпоративною інформаційною безпекою. *Економіка та суспільство*, (43). 2022. https://doi.org/10.32782/2524-0072/2022-43-49

14. Бржевська З. М., Гайдур Г. І., & Аносов А. О. Вплив на достовірність інформації як загроза для інформаційного простору. *Кібербезпека: освіта, наука, техніка*, (2), 2018. С.105-112. https://doi.org/10.28925/2663-4023.2018.2.105112

15. Куліковський А. Технологія Blockchain як складова інформаційної безпеки. *Кібербезпека: освіта, наука, техніка*, 4(4), 2019. С.85-89. https://doi.org/10.28925/2663-4023.2019.4.8589

16. Кравченко О. М. Удосконалення охорони комерційної таємниці та конфіденційної інформації в Україні для інтеграції в Європейське бізнес-середовище. *Нове українське право*, 1, 2022. С.211-220. https://doi.org/10.51989/NUL.2022.6.1.29

17. Савицька Л., Коробейнікова Т., Волос О., & Тарновський М. Метод та засіб моніторингу безпеки в комп'ютерній мережі засобами SIEM, *ІТКІ*, вип. 58, вип. 3, с. 22–32, Груд 2023. https://doi.org/10.31649/1999-9941-2023-58-3-22-32

18. Гребенник А. Г., Трунова О. В., Казимир В. В., & Міщенко М. В. Виявлення та прогнозування рівня загроз для корпоративної комп'ютерної мережі. *Технічні науки та технології*, (2 (20)), 2020. С.175-185. https://doi.org/10.25140/2411-5363-2020-2(20)-175-185

19. Кошара А. В., & Бакало Б. В. Підвищення захищеності державного сектору на основі SIEM-систем. *Інфокомунікаційні та комп'ютерні технології*, 2(04), 2022. С.128-133. https://doi.org/10.36994/2788-5518-2022-02-04-14

References:

1. Sheeraz M., Paracha M., Haque M., Durad M. and oth. (2023). Effective Security Monitoring Using Efficient SIEM Architecture. *Human-centric Computing and Information Sciences*, vol.13, Article number 23, 2023. https://doi.org/10.22967/HCIS.2023.13.023

2. Kozak M., Plichta A. (2025). Implementation of a SIEM System Using Splunk and the Enterprise Security Module and Analysis of Its Effectiveness in Detecting Cyber Threats. Proceedings of Conference: 39th ECMS International Conference on Modelling and Simulation, vol. 39, is. 1, 2025. https://doi.org/10.7148/2025-0269

3. Okamoto H. (2021). The Role of Information Security Event Management (SIEM) in Enhancing Intrusion Detection and Cybersecurity Through Machine Learning Technology. https://doi.org/10.13140/RG.2.2.35096.00003

4. Dergaliuk B. V. (2023). Vplyv tsyfrovoyi transformatsiyi na zabezpechennya ekonomichnoyi bezpeky pidpryyemstva [The impact of digital transformation on ensuring the economic security of an enterprise]. *Economic Bulletin of the National Technical University of Ukraine "Kyiv Polytechnic Institute,"* (26), 65–68. https://doi.org/10.20535/2307-5651.26.2023.287057 [in Ukrainian]

5. Kramarenko I. S., Irtyshcheva I. O., Bilousova S. V., Irtyshchev O. S., & Harahulia A. V. (2024). Orhanizatsiyno-upravlins′ki mekhanizmy zabezpechennya informatsiynoyi bezpeky pidpryyemnyts′koyi diyal′nosti v umovakh tsyfrovoyi transformatsiyi ekonomiky Ukrayiny

[Organizational and managerial mechanisms for ensuring information security of entrepreneurial activity in the context of digital transformation of Ukraine's economy]. *Entrepreneurship and Innovation*, (32), 246–252. https://doi.org/10.32782/2415-3583/32.38 [in Ukrainian]

6. Polova N., Kohut R., & Duma Yu. (2024). Napryamy zabezpechennya bezpeky pidpryyemstva v umovakh tsyfrovizatsiyi biznesu [Directions for ensuring enterprise security in the context of business digitalization]. *City Development*, 1(01), 90–94. https://doi.org/10.32782/city-development.2024.1-12 [in Ukrainian]

7. Shevchuk A. A. (2024). Zakhyst tsyfrovoho aktyvu z vykorystannyam SHI – osnova bezpeky krayiny ta efektyvnist′ upravlinnya biznes protsesamy v umovakh tsyfrovizatsiyi. [Protection of digital assets using AI as a basis for national security and effective management of business processes in digitalization conditions]. *Tsyfrova ekonomika ta ekonomichna bezpeka*, 3(12), 41–46.

https://doi.org/10.32782/dees.12-7 [in Ukrainian]

8. Lehominova S. V., Shchavinskyi Yu. V., & Budzynskyi O. V. (2024). Analiz suchasnykh pidkhodiv do zabezpechennya kiberbezpeky korporatyvnykh baz danykh [Analysis of modern approaches to ensuring cybersecurity of corporate databases]. *Modern Information Protection*, (2), 50–58. https://doi.org/10.31673/2409-7292.2024.020006 [in Ukrainian]

9. Bondarchuk O. I., Naumenko T. S., & Tovt B. M. (2024). Rozrobka ta vprovadzhennya innovatsiynykh metodiv kiberbezpeky u komp″yuternykh systemakh. [Development and implementation of innovative methods of cybersecurity in computer systems]. *Tavria Scientific Bulletin*. Series: Technical Sciences, (4), 31–40. https://doi.org/10.32782/tnv-tech.2024.4.3 [in Ukrainian]

10. Bakalinska O. (2022). Suchasni tendentsiyi pravovoho rehulyuvannya kiberbezpeky ta intelektual′na vlasnist′ [Current trends in legal regulation of cybersecurity and intellectual property]. *Teoriya i praktyka intelektual'noyi vlasnosti*. (5), 82–92. Retrieved from URL: https://coordynata.com.ua/sucasni-tendencii-pravovogo-reguluvanna-kiberbezpeki-ta-intelektualna-vlasnist [in Ukrainian]

11. Androshchuk H. (2017). Intelektual′na vlasnist′ v systemi internet rechey: ekonomiko-pravovyy aspekt [Intellectual property in the Internet of Things system: Economic and legal aspect]. *Teoriya i praktyka intelektual'noyi vlasnosti*, (6). Retrieved from URL: https://drive.google.com/file/d/1lytw_L95SQuvdNa8-d3DbMvQ51P0hmeW/view [in Ukrainian]

12. Kalashnikova L. V., & Yarova L. (2023). Tsyfrovizatsiya sotsial′nykh vidnosyn: teoretychne obhruntuvannya ta empirychna veryfikatsiya [Digitalization of social relations: Theoretical justification and empirical verification. Karavela. Retrieved from http://elibrary.kdpu.edu.ua/xmlui/handle/123456789/10687 [in Ukrainian]

13. Chubaievskyi V. (2022). Metody upravlinnya korporatyvnoyu informatsiynoyu bezpekoyu [Methods of corporate information security management]. *Economy and Society*, (43). https://doi.org/10.32782/2524-0072/2022-43-49 [in Ukrainian]

14. Brzhevska Z. M., Haidur H. I., & Anosov A. O. (2018). Vplyv na dostovirnist′ informatsiyi yak zahroza dlya informatsiynoho prostoru [Impact on information reliability as a threat to the information space]. *Cybersecurity: Education, Science, Technology*, (2), 105–112. https://doi.org/10.28925/2663-4023.2018.2.105112 [in Ukrainian]

15. Kulikovskyi A. (2019). Tekhnolohiya Blockchain yak skladova informatsiynoyi bezpeky [Blockchain technology as a component of information security]. *Cybersecurity: Education, Science, Technology*, 4(4), 85–89. https://doi.org/10.28925/2663-4023.2019.4.8589 [in Ukrainian]

16. Kravchenko O. M. (2022). Udoskonalennya okhorony komertsiynoyi tayemnytsi ta konfidentsiynoyi informatsiyi v Ukrayini dlya intehratsiyi v Yevropeys′ke biznes-seredovyshche [Improvement of trade secret and confidential information protection in Ukraine for integration into the European business environment]. *New Ukrainian Law*, 1, 211–220. https://doi.org/10.51989/NUL.2022.6.1.29 [in Ukrainian]

17. Savytska L., Korobeinykova T., Volos O., & Tarnovskyi M. (2023). Metod ta zasib monitorynhu bezpeky v komp″yuterniy merezhi zasobamy SIEM [Method and tool for network security monitoring using SIEM] systems. *Information Technologies and Computer Engineering*, 58(3), 22–32. https://doi.org/10.31649/1999-9941-2023-58-3-22-32 [in Ukrainian]

18. Hrebenyk A. H., Trunova O. V., Kazymyr V. V., & Mishchenko M. V. (2020). Vyyavlennya ta prohnozuvannya rivnya zahroz dlya korporatyvnoyi komp″yuternoyi merezhi [Detection and forecasting of threat levels for corporate computer networks]. *Technical Sciences and Technologies*, 2(20), 175–185. https://doi.org/10.25140/2411-5363-2020-2(20)-175-185 [in Ukrainian]

19. Koshara A. V., & Bakalo B. V. (2022). Pidvyshchennya zakhyshchenosti derzhavnoho sektoru na osnovi SIEM-system [Improving public sector protection based on SIEM systems]. *Infocommunication and Computer Technologies*, 2(04), 128–133. https://doi.org/10.36994/2788-5518-2022-02-04-14 [in Ukrainian]

© О. А. Нємкова, Т. І. Коробейнікова, М. К. Русинко, С. Т. Масник, 2026.
Науково-методична стаття.
Надійшла до редакції 18.11.2025.
Прийнята до друку 29.04.2026.
Опублікована 25.05.2026.